Unorthodox Thoughts about Asymmetric Warfare

MONTGOMERY C. MEIGS

"Bad terminology is the enemy of good thinking."
— Warren Buffett[1]

In the last few years the use of nerve agent in the Tokyo subway by Aum Shinrikyo and al Qaeda's offensive leading to its 9/11 attacks on the World Trade Center and the Pentagon forced us to reevaluate the threat of terrorism to our art of operations. As a term of art, asymmetric warfare now dominates public attention. But many use the term with little understanding of its operational meaning. In this new strategic environment we had best heed the admonition of Mr. Buffett, the Sage of Omaha, and agree on a set of definitions that will provide our tools for analysis. In preempting the terrorist are we really dealing with asymmetry, or is something else at work? Thinking of the threat as only asymmetric misses the mark, especially if we have the concept wrong. The combination of asymmetry and the terrorists' ability continually to devise idiosyncratic approaches presents our real challenge. Assessing the distinction and interrelationship between these two factors provides us with the initial understanding required to address the operational challenges.

Asymmetry means the absence of a common basis of comparison in respect to a quality, or in operational terms, a capability. Idiosyncrasy has a different connotation—possessing a peculiar or eccentric pattern. In a military sense, idiosyncrasy connotes an unorthodox approach or means of applying a capability, one that does not follow the rules and is peculiar in a sinister sense.

Actually, al Qaeda's overall strategy is not new. In the 11th and 12th centuries the Assassins, a militarily weak fundamentalist and extremist sect, used pinpoint killing to bring more powerful ruling groups to heel. Indoctrinating their young followers into an extreme and enthusiastic cult of Shiite Islam, they sent individuals and small teams out to infiltrate the inner circles of targeted

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Unorthodox Thoughts about Asymmetric Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,122 Forbes Avenue,Carlisle,PA,17013-5244**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Parameters, US Army War College Quarterly, Summer 2003, Vol 33, No. 2

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

leaders. These zealots worked their way into the retinue of the targeted official by gaining trusted status as a groom, guard, or servant. When close enough to the target and with no regard for their own survival, they murdered their prey with the dagger given them by their leader. The Assassins even managed to threaten Sal al Din the Kurd, the commander who drove the Crusaders out of Palestine. After Sal al Din's mail shirt foiled the first attempt, while on campaign a wooden tower was built in his camp to provide him a safe resting place. For the Assassins, dying in the attempt mattered not, since their ascension into paradise was assured.[2] Sound familiar?

Today, only the mechanism of attack has changed. Dispatching individuals or small teams with a mission to painstakingly infiltrate and develop an opportunity for attack remains a part of al Qaeda's technique. Instead of penetrating the structures within the palace of the ruler or the retinue of followers in the camp of a general, terrorist agents now weave their slow, purposeful way through international systems of education, commerce, and travel, accessing the fabric of democratic societies and exploiting our freedom of movement, information systems, protection of civil rights, and the general laxness in our public security. Instead of a dagger, al Qaeda's infiltrators began with explosives and then discovered how to reverse-engineer the technological mechanisms of modern society in highly destructive and murderous ways. Given our societal dependence on interconnected, technologically intensive systems, al Qaeda used asymmetric means to cleverly develop idiosyncratic attacks on its targets, thus changing our operational and strategic environment.

History of Asymmetric Warfare

To isolate al Qaeda's true advantage, we should begin with a look at the historical roots of asymmetric warfare. Military affairs are replete with campaigns won by forces with capabilities similar, though different by degree, to those of their opponents. True examples of operational and strategic asymmetry are relatively rare. Technological, operational, and tactical innovation combine to create them. As a basis for measuring technological innovation today, many

---

General Montgomery C. Meigs (USA, Ret.) the former Commander of US Army Europe and 7th Army, is the Distinguished Visiting Tom Slick Professor of World Peace at the LBJ School of Public Policy, University of Texas, Austin. Early in his career he served as a company-grade officer in command of armored cavalry units in Germany and Vietnam. After study at the University of Wisconsin-Madison he taught history at the US Military Academy, and he subsequently received his doctorate in history from Wisconsin in 1982. His commands have included 1st Squadron, 1st Armored Cavalry Regiment; the 2d Brigade, 1st Armored Division in Operation Desert Storm; and the 3d Infantry Division until its reflagging as the 1st Infantry Division in February 1996. In October 1996 he deployed with the 1st Infantry Division to Bosnia as Commander of Task Force Eagle and NATO Multi-National Division (North). He returned to Bosnia in November 1998 as Commander of the NATO Stabilization Force (SFOR).

---

cite the German offensive into France in 1940, the so-called blitzkrieg, as asymmetric warfare. It was not.

The German attack on France in 1940 provides a useful example of the collapse of political will as a result of a disastrous campaign, but not the use of asymmetric warfare. The strategic differences between the French and Germans in 1940 involved organization, planning, and political will. The French plan of campaign placed many of their best troops deep in the Maginot Line forts. They then moved their crack maneuver forces into Belgium to counter the reprise of the Schlieffen Plan they expected on that axis. The 1940 German plan entailed an attack into the Low Countries designed to draw the French into a meeting engagement in Belgium. The German armored spearhead drove through the Ardennes at Sedan, the hinge in the French line between the Maginot Line and the French and British armies advancing into Belgium. Only second-rate, newly deployed units defended this essential linchpin in the French operation. The German blow fell precisely on the most poorly defended spot.

The memory of the losses in the First World War traumatized the French generals. It sapped their resolve, draining from them any sense of innovation or sufficient intellectual ability to react in the 1930s to the growing capability of the Wehrmacht. Nor did French leaders study the German successes in Poland. Faced with the German occupation of the Ruhr, then the Anschluss, the Munich crisis, and then the German invasion of Norway, French leaders tabled difficulty after difficulty in councils of war, always recommending to their political chiefs accommodation and never the use of force, even when they had tremendous advantages early in the conflict. The tumultuous politics of the 1930s left the French body politic torn between the forces of the right and left. The connivance of the 200 richest families, none willing to look past its psychological fatigue and warped self-interest to appreciate the good of the state, devastated political will.

The Wehrmacht actually had no tactical or operational weapon systems incomparable to those of the French or unknown to them. The French had the better tank. They had numbers of combat aircraft and pilots comparable to the Luftwaffe, which in the air-to-air combat over Holland and Belgium gave a good account of themselves. In the late 1930s French military thinkers like General J. B. E. Estienne and then-Colonel Charles de Gaulle argued for the type of mechanized units adopted by the Germans. They also advocated using aircraft and armored formations in tactics similar to those adopted by the Wehrmacht. They understood the purpose of close air support at the point of attack. Fixed on their experiences in the World War I trench fighting, however, the French senior generals rejected these ideas in favor of a doctrine derived from the tactics of infantry defense, allocation of artillery fires, parceling out their armor, and relying on the telephone for command and control.

Differences in degree of capability—but not asymmetries—existed between French and German units at the tactical level as well. The German units were simply better, especially at the critical point in the campaign on the Meuse

at Sedan where Guderian's armored divisions met the French 55th and 71st Infantry Divisions. The Germans' theory and practice of maneuver warfare integrated aircraft, signal, armor, and artillery into a combined-arms force oriented on exploitation, versus the French emphasis on static infantry defense. Their commanders led aggressively at the point of attack. French leaders remained in their command posts, far from the fighting, attempting to control quickly developing situations over telephone lines subject to interdiction by artillery fires and bombing. The Germans massed their armor into ten divisions with a corps focused directly on the hinge at Sedan. Actually, German infantry and engineers forced the breakthroughs across the Meuse using tactics not unlike those in World War I. The armor followed and then exploited the penetration ruthlessly.

The Germans accepted risk to generate cascading reverses, collapsing the French army's ability to respond. But these kinds of paralyzing pursuits are not unprecedented in history. Murat after Jena and Auerstadt rode the Prussian army to ground. Grant and Sheridan did the same thing to the Army of Northern Virginia after Five Forks. Advised by old, worn out, feckless generals reacting to the scars of the trenches at Verdun, without the will to persist and themselves trapped in a political system unsure of the validity of its own survival, the political leadership of the Third Republic crumbled.[3]

Yet none of the German weapons or techniques were in any way "lacking a common basis of comparison" to those of the French. The French leadership squandered the technological lead it held in 1918. French generals hamstrung their forces with inadequate doctrine, poor training, uncourageous leadership in the field and in the corridors of power, and a flawed plan of campaign that offered opportunity exactly where the Germans attempted to seize it. Errors strategic and operational, differences in tactical skill, and operational planning all contributed to French collapse and German success—but not asymmetry.

The best recent example of operational asymmetry involves the US campaign in Afghanistan. US forces entered the fray with technological superiority in sensors and space-based communications and the ability to deliver precision weapons from aircraft. Based on training, initiative, and fieldcraft, they possessed the ability to knit together new tactical techniques integrating an air operation and special forces with an indigenous formation, the Northern Alliance. This combination, developed after forces were engaged, created a unique operational advantage. Once the ground formations of the Northern Alliance were linked by Special Forces teams providing precise and timely targeting data to attacking aircraft, this resulting asymmetry denied Taliban forces the ability to control or defend key terrain. By exacting a great price on the Taliban for any massing of forces to defend or counterattack, the asymmetrical advantage of the US ground-based targeting and air attack made the ground forces of the Northern Alliance unstoppable. The Taliban and al Qaeda had nothing of comparable capability with which to oppose the US advantage.

After their defeat, when the Taliban and al Qaeda forces broke apart and exfiltrated into the mountains of Pakistan and into the villages of remote Afghanistan, they removed the US advantage. Then the comparative force capabilities returned to a situation very familiar to Afghan fighters over the centuries, a relatively conventional military force on the ground attempting to chase down groups and individuals almost invisible in the native culture and terrain. Now what is left of the Taliban snipes at the international effort and the government in power in Afghanistan. At this point in time al Qaeda presents a more dangerous problem with regard to how we frame the strategic challenge.

Idiosyncratic Attack

Our problem does not only involve forces in the field. One lesson of 9/11 is that al Qaeda now applies additional idiosyncratic threats to the operational structures of campaigns as well as to strategic targets. Operational asymmetry is important when military capabilities are employed. But today's threat from terrorism and the type of operations we can expect from terrorist networks in the future derive from idiosyncratic uses of both military and nonmilitary capabilities. At the lower end of the spectrum of violence, we find idiosyncratic approaches posing tremendous threats to operational and national targets alike. By attacking idiosyncratically at a point the enemy selects in an attempt to avoid US operational advantages, and by exploiting our weaknesses or blind spots, the terrorist is capable of inflicting harm at will. His operational asymmetry is derived from his ability to continuously evolve new tactics and by the cellular and compartmented nature of his support structures. To this organization he adds a continuing flow of new, idiosyncratic means of attack. His advantage lies in our inability to recognize these new structures of his operation and to predict his new attack vector.

This problem requires a different method of analysis and organization of forces as opposed to those relevant to conventional military operations. While our current military capability must focus on preparation for the challenges of a major war in which operational tasks are fairly well known ahead of time, US planners must simultaneously prepare to operate in contingency operations like those in Afghanistan or the Balkans. In these unconventional settings, conflict usually begins with little warning. As in Afghanistan, the operational techniques needed to win may have to be invented after the unit deploys and is operationally engaged. Ironically, peace enforcement or peace-making can entail intermittent levels of violence awfully close to what we consider mid- to high-intensity conflict. The mission sets are normally more abstract and involve a fleeting and indistinct enemy wed to nonmilitary support structures.

Technology plays a critical role in this new equation. Strategically, from financial markets to transportation systems to electric power grids, standards of living worldwide depend fundamentally on integrated technical systems that are susceptible to idiosyncratic threats. The operational structures upon which cam-

paigns depend have similar attributes. These systems may have internal safeguards against failure in normal operations, but they do not have an ability to avoid catastrophic failure when they are interrupted or attacked in an unexpected, unanticipated, and peculiar way that generates cascading or accelerating effects.

The Northeast blackout of 9 November 1965 provides a useful example. At 5:16 p.m. on that day, an overcurrent relay on a transmission line from the Beck power plant outside of Toronto tripped and shut down one of six lines carrying power from that plant into the Canadian power grid that served Ontario. In 2.5 seconds—to protect Beck's generators from overload—shutdowns rippled through the Canadian system, closing off the five other lines from the plant. The transmission systems in Ontario were linked to systems in New York. When the demand from Ontario went off-line, Beck's output surged into the power grid in New York, almost doubling throughput. The overload began to surge through the US grid, threatening generation plants all over the Northeast. To protect their own generators, private utilities took their systems off-line, forcing the large public utilities to follow suit. In a total of four seconds, the Northeast went completely dark.[4] The blackout represents the potential for catastrophic failure of technologically intensive systems with high degrees of interdependence. If one can find a weakness through which safety factors can be overloaded or bypassed, then manipulate the system in a self-destructive, eccentric manner, he can cause imploding, catastrophic failure.

The principle also applies in military operations. If one can attack the center of gravity of an operational system in an idiosyncratic manner with weapons or a combination of weapon systems that the opponent does not possess—or, even better, does not even understand or perceive—then the perpetrator can achieve catastrophic failure of that system, whether the target is a transportation network or an integrated command and control grid. The potential effect increases to the degree that the system is technologically intensive and functionally or geographically integrated.

Additionally, the use of weaponry that is asymmetric to the capabilities of the opponent and applied idiosyncratically creates a special problem. Al Qaeda's attack on the World Trade Center and the Pentagon provides the most recent and spectacular example. If one thinks of a modern passenger plane in terms of its explosive and incendiary potential, one has a guided missile of devastating effect. The airlines' easy ticketing, passenger handling, and access to the cockpit became an idiosyncratic axis of approach to the target. The combination permitted the terrorists to use a mechanism for transportation we all take for granted as part of our system of commerce and common benefit, and turn it into a devastating weapon. In bin Laden's words, on a videotape captured in Afghanistan,

> We calculated in advance the number of casualties from the enemy, who would be killed based on the position of the tower. We calculated that the floors that would be hit would be three or four floors. I was the most optimistic of them all. . . . Due to my

> experience in this field, I was thinking that the fire from the gas in the plane would melt the iron structure of the building and collapse the area that the plane hit and all the floors above it only. This is all we had hoped for.[5]

The asymmetry in this case stems not from weaponry, but from the unique, one-time cellular teams and support structure formed for this particular operation, combined with stealth and surprise, and culminating in an idiosyncratic approach by terrorists inserting themselves into the cockpits of airliners. Any future attacks may involve another type of team evolved specially for its own type of stealthy attack, with another combination of support and command links back to al Qaeda or some other yet-to-be-derived informal organization. This method has strategic import in terms of the vulnerability of national or operational targets. The attack on the World Trade Center towers and the Pentagon used only a handful of infiltrators and cost about $500,000.[6] This attack method was unique, indeed not even comparable to anything that had been attempted before.

Al Qaeda's true operational asymmetry derives from its ability to change its operational system at will in response to the methods needed to approach and attack each new target. First, we saw attacks on embassies with car bombs, next the use of an explosive-laden dinghy to cripple USS *Cole*, and finally the perversion of the function of a passenger aircraft to produce a human-guided missile. Al Qaeda adapted a new form of organization in each case, a structure optimized for the differing environments of the separate targets. Simultaneously, due to other pressures, they also relocated their base for command and logistics from the Sudan to Afghanistan. Operation Enduring Freedom then forced them to move again. The nexus of the problem involves divining and preempting the creativity of an unconventional opponent and his ability to reform and reorganize in an effort to create new structures for command and control and new attack mechanisms exploiting idiosyncratic approaches to his target. This problem exists for the operational and logistical structures we deploy to conduct campaigns as well as for systemic strategic targets in our national civil structure and in those of our allies.

Technology and Terrorists

Now that the unconventional threat is so closely linked to national defense, military leaders must be trained to recognize the wider problem. Military organizations must be able to work across a much broader field of activities than those of the conventional military setting. The merging of conventional and unconventional capability and the ability of terrorists to strike at the operational and strategic levels demand a new doctrinal context. The military cannot be saved to only fight the next world war. Leaders need to be trained to recognize the warning signs and to expand their approaches to this new environment. We must provide them the tools to prevent the benefits of unconventional conflict by adapting to the current reality.

Other factors complicate our challenge. The information revolution creates new difficulties for our national decisionmakers and for their intelligence officers. Modern encryption easily available in the public domain gives anyone with internet access the ability to encrypt their personal communications with keys that are virtually impossible to break. As their use becomes more widespread, prioritizing efforts to isolate and focus on criminal, terrorist, or military applications becomes extremely difficult. More and more, the terrorist or an opposing military can communicate with impunity via commercial channels. The time value of intelligence thus decays quickly. In the growing sea of bits, finding and getting to the relevant information takes significantly more time, effort, and money. No longer must the spy, terrorist, criminal, or rogue paramilitary develop his own secure and stealthy means of communication. Instead, they can wrap themselves in 128- or 512-bit encryption, knowing that if they act quickly the intelligence value of the content of their communications will decay, usually well before they can be caught.

As Abdullah Muntazir, the spokesman for Pakistan's Lashkar-e-Taiba, an Arab group with its origin in Afghanistan focused on consolidating Kashmir, remarked to Peter L. Bergen, "This technology is a good thing."[7] For non-state actors and terrorists, the availability of off-the-shelf information technology at low cost allows a very powerful combination of the tribal and the technological. A self-healing, cellular system based on group or familial ties with personal identification tied to group affiliation or shared experiences makes the work of the intelligence agency fiendishly difficult. Templating and predicting the actions of cellular terrorist networks that constantly change and reform from fragments of the old structure becomes a shot in the dark. This is especially true as each successive attack seeks to employ a different idiosyncratic approach to the target and perhaps using a different organizational structure or unprecedented attack mechanism.[8] Individuals and small teams move like microbes through the veins of the transportation systems in democracies. They are able to use modern society's central nervous system of unprotected information networks to regenerate and recombine, forming temporary links to the compartmented system of command and logistics that supports the terrorist network. Undetected, they develop novel attacks. This capability presents a new and perplexing problem.

Moral conviction and conventional military efficiency alone will not allow us to understand and counter a threat that attacks society and its operational structures through its own circulatory and nervous systems, striking by short-circuiting our highly integrated and technologically integrated structures. We must be equally as innovative and intuitive in our effort to get the strategy right. We face the challenge of developing a concept of operational art that is capable of countering the asymmetries of an opponent who uses the theater of unconventional warfare to achieve non-state objectives against nation-states.

How then can we foster an art of operations that facilitates attacks on the transnational structure of al Qaeda and assists other nations in resolving their

own internal problems with national groups having links to international terrorism? While addressing this new threat, we must also maintain a force capable of winning in high-intensity conflict, and that raises another issue: How do we counter a threat that seeks to obviate the advantages we possess in conventional military power?[9]

To respond properly, we need to address the full range of military activity associated with unconventional warfare. Countering asymmetry and idiosyncrasy in a setting that is so conducive to their efforts requires an atypical approach. If asymmetric warfare in this context involves an enemy's ability to constantly change form and method at will from the fragments of the old operation and recruiting base, then we need to look for signs of his new operational shape as well as the emergence of new families of capability—conventional and unconventional.

This response will require tremendous creativity. We need to first ask ourselves how our enemy might change his operational structure, his actual organization, in an attempt to accomplish his ends. Then we need to ask in what areas might he develop superior knowledge or some unprecedented, perverted use of a capability. For instance, in the case of a terrorist group, if we improve our ability to see them as they move about, how will their system allow them to adopt a new form? Where are the disconnected internal fragments and the essential communications nodes? From where will new teams come? It is to our advantage to recognize how the enemy's ability varies from target environment to target environment. What boundaries will he cross today, and then, as we feel him change, tomorrow? We must ask ourselves what capabilities our adversaries have that we do not understand or expect. What are the links to organized crime and how can we counter that source of assistance? Terrorists will adapt lawful capabilities from the public domain, or purloin them from secure areas, and combine them in ways that are unprecedented and destructive. How do we anticipate their ability to innovate?

Exposing asymmetry goes hand in hand with isolating opportunities for idiosyncrasy. Our military, police, and scientific communities understand the capabilities that terrorists could exploit to produce mass effects. The problem involves the unprecedented and eccentric ways that substances or mechanisms of destruction may be delivered. Highly radioactive isotopes in a conventional suitcase bomb or biological agents disseminated by an aerosol are not unknown, but the eccentric means of delivery could be. So the question asked to spur the queries in the intelligence and law enforcement communities becomes quite different. Point defense is only a last resort. How do we recognize and preempt our opponents' idiosyncratic approach? There may be back doors that we are not watching—isolated harbors, off-corridor air access for small planes to cross our borders, or rural land crossing points. Or the opponents may use agents already inside the country. In a campaign setting, for instance, how do we verify the trustworthiness of contractor employees from the host nation?

These threats to our national systems apply as well to the structural elements that make up military forces in the field. We must ask ourselves where our interdependent, highly integrated, and technologically intensive systems are most at risk. How are logistics and communications most susceptible to manipulation in a way that could produce catastrophic effects? Where are our forces most vulnerable—in transit, in staging, in onward movement? In both the national infrastructure and in the military infrastructure in the field, what are the vulnerabilities where an eccentric attack could begin a process of accelerating destruction? How do we protect those vulnerable points? We need to emplace in those systems safety measures that will ensure the system can diagnose failure and initiate either a healing response or a local shutdown that isolates the problem. For instance, in space-based communications structures, can we rely on commercial systems which our opponents might access, or do we need to invest substantial sums to procure a national capability used only for military communications? In such cases we may have to find an acceptable balance between risk and cost.

Not too surprisingly, assessing asymmetry and idiosyncrasy as separate but linked aspects of the larger problem leads to a new framework for the art of operations. Addressing asymmetry in the context of counterterrorism requires an inquiry that attempts to identify evolving organizational structures and capabilities not yet seen—either a new structure for attack or modifications the enemy has made to known weapons or capabilities. In the case of al Qaeda, we must focus on their ability to assume a new cellular form from parts still available but unseen in the operational environment. On the other hand, addressing idiosyncrasy requires rigorous assessment of functional systems within our own military organizations and in the structures of society as they relate to families of weapons or operating structures of a prospective opponent. We need to identify our own systemic weaknesses and envision how the enemy will attack via these avenues. Why would a potential enemy try to sink a ship at sea when it is so vulnerable in port?

Meeting the Challenge

To address the challenges of this new strategic environment, we should stop rejecting the lessons of contingency operations conducted during the last ten years. Our Vietnam experience and its aftermath left in the hearts and minds of many military leaders an aversion to anything falling outside classical operational tasks—for instance, nation-building. But we have had units operating in the new world that was exploited by al Qaeda for at least a decade. Ironically, the desire to maintain the highest possible readiness for high-intensity conflict has in part disguised a reluctance to accept a return to the potentially contaminating environment of low-intensity conflict, even while our troops were operating in that environment. The spectrum of violence is continuous. There should not be a discontinuity between theory and military practice in a world in which our military will be summoned, with little warning, to operate throughout the entire spectrum.

Our doctrine and training need to be modified to reflect the lessons units have learned in the tough realities of campaigning in Bosnia, Kosovo, Southwest Asia, Haiti, Panama, and Afghanistan, as well as in larger operations like the war on Iraq. Our operational concepts of military efficiency should be adapted to reflect this new strategic framework. New concepts of military efficiency begin with intelligence and decision theory and end with organization and training.

The analytical system for unraveling threats of asymmetric capabilities applied idiosyncratically to vulnerabilities in our military and economic systems requires a new form of hybrid intelligence. As in Bosnia-Herzegovina, where a combination of military and civilian intelligence operators produced the insights that allowed the Stabilization Force to apprehend al Qaeda operators shortly after 9/11, we need capabilities for collection management and fusion at the operational level that work across institutionally derived bureaucratic fault lines. In unconventional warfare as well as counterterrorism, the military, US Customs Service, Federal Bureau of Investigation (FBI), Internal Revenue Service, Immigration and Naturalization Service (INS), Coast Guard, Treasury, Federal Aviation Agency, and other specifically focused organizations all possess unique capabilities for looking at the phenomena that occur in their areas of expertise. Sometimes the information they glean derives from the public domain. Sometimes it must be gathered clandestinely by the most subtle and fragile means. But each agency views the operational phenomena differently. Often the information must be interpreted by linguists or others familiar with the particular culture from which the information originates.

Unless we can place in the field, in immediate support of the commander of the campaign, structures that obviate the boundaries of organizational culture and turf and fuse intelligence across disciplines, we risk overlooking important individual components as well as missing the big picture. Our analysts have to be provided an environment where they can work together productively. Immersing combinations of experts from the different disciplines in the operational problem and motivating them to find solutions under pressure will be essential. It offers the only way to create a new social architecture matched to the problem that can achieve the hybrid situational awareness and analytical acuity we require. This integrated communication, "brings to the performance of the function the knowledge necessary for its successful execution"—in this case the relevant intelligence picture in time.[10]

We also need to change the mix of minds that generate intelligence requirements. We must incorporate unorthodox thinkers who probe constantly for the unique and peculiar danger or method of access. This kind of training should be part of the professional development of our planners and commanders. We need to build into the system thinkers who ask the question no one else considered or dared to ask. In addition we should include scientific advice to help isolate critical nodes in our integrated systems where an enemy might initiate a chain of destruction. Along with the normal threat-based questions, these kinds

of thinkers will drive the intelligence managers to look for the previously unanticipated, the peculiar or unique, and task across all agencies for critical, anomalous bits of information.

In the analysis of raw information and its fusion into the actionable intelligence upon which decisionmakers must depend for preemptive action, we need to include in the analytical organization representatives of all the agencies relevant to the problem. If we are dealing with cross-border infiltration of paramilitaries assisted by international structures of organized crime, the fusion cell should include representatives from Treasury, FBI, Customs, and other national agencies capable of highlighting and describing their piece of the puzzle. Such operators should be detailed by the National Command Authorities (or conceivably by the Department of Homeland Security) to the joint task force as a national priority at the outset of the campaign in a way that makes them loyal to the common endeavor. Their tenure must be long enough for them to learn the situation at hand and to establish trust with and confidence in their teammates. They must have access to the intelligence systems and databases of their host agency as well as competence in their discipline and the seniority in their home office to allow them to move about in its systems to gain the information needed.

Finally, we need to improve our means for collecting human intelligence (humint). In operations in Bosnia, for instance, time and again critical actionable intelligence came from Army humint teams. Where strategic systems often failed to give the "granularity" or level of detail that operators required, relatively unsophisticated elements operating in the open with a sensitivity to the environment and their noses to the ground provided better and more timely insights than all the input of national strategic systems. To face the new asymmetric and idiosyncratic threat, we must improve our capacity for acquiring human intelligence.

Executing decisions based on better intelligence depends on having units organized and trained for this new operational setting. Now that the threat to national interests and systems from low-intensity conflict is severe, focusing units intensely on the tasks needed to win in conventional combat is no longer sufficient for operational success across the spectrum of conflict. Granted, high-intensity conflict continues to pose the most deadly challenge our units face. Losing a war would bring dreadful consequences to our nation, but so would the use of a weapon of mass destruction in a major population center or at a key transportation node in a theater of operations.

Readiness for the kinds of stresses we anticipate in high-intensity combat will continue to demand first priority in our training. Fortunately, many of the tasks and disciplines needed at the company and platoon levels in high-intensity conflict also apply to operations in an unconventional setting. Keeping units intensely ready for conventional operations maintains unit tactical skills relevant to the unconventional setting.

But the absence of peer competitors that would seek to contest our advantages in conventional capability lessens the likelihood of high-intensity conflict. Our challenge then is to develop an organizational concept that spans the two dimensions. We must continue to possess the forces and systems we need to provide conventional deterrence and, if deterrence fails, to win decisively. As they have been doing in low-intensity conflicts for the last decade, however, these same units must also be able to task organize on short warning into new structures to defeat opponents who seek to apply asymmetrical abilities in idiosyncratic approaches in unconventional settings. To be able to accomplish both of these missions, units must maintain a sophisticated level of training. As our Special Forces soldiers did in Operation Enduring Freedom, and as conventional units did in Bosnia, Kosovo, and Iraq, they must also be able during a campaign to improvise from established doctrine to develop new tactics and techniques.

Continuing to attain this type of force depends on maximizing several operational capabilities. The ratio of leaders to led should be increased. Asking a unit to prepare for dissimilar tasks simultaneously and to be able to move on short notice to accomplish a range of operational missions, some for the first time, requires a high level of experience and individual competence. Soldiers have to be physically and emotionally mature, and there should be a higher density of experienced leaders in the formation. Opposed force training should be more frequent and intense. While drills are important for any teams performing collective tasks, we need to enhance the entrepreneurial ability of our units in an operational sense. No longer should we measure readiness by miles driven or hours flown, but by a rigorous assessment of tasks accomplished to the standard needed to succeed in the field and to support innovation in the field. If we need to fly more hours and maneuver more miles to attain the levels of proficiency needed to meet the two sets of mission-essential tasks, we should resource that training or operational tempo—and provide the quality of life for families needed to support the pace. If we need additional combat training centers to provide the more frequent training opportunities required to master the challenges of the Army's contemporary operational environment, we should invest in them.

If we get the structure for command and decision right, new dimensions of capability will derive from related civilian developments in information technologies as they apply to precision and accessible situational awareness. Civilian firms will continue to innovate at a rate enabled by Moore's Law,[11] which states that the number of transistors per square inch on a chip, a measure of computing power, doubles every year—now actually every 18 months. Industry will continue to exploit new chip technology, providing greater capabilities for command and control by incorporating advances in sensors and information processing. To take full advantage, we need to find a way to break the tyranny of the military's five- to ten-year development cycle and incorporate new C4ISR[12] capabilities into our formations at a rhythm matched to the reality of commercial innovation. As advances come from the civilian sector in a nine- to 18-month cycle, we need

to be able to incorporate the relevant results immediately across the appropriate echelons of our formations. We cannot wait five years for some imagined perfect technology. Our opponents surely will not. By purchasing civilian equipment off the shelf, our opponents may be able to deploy a greater capability than we can provide to our own units.

In addition, just as Moore's Law enables exponential increases in speed and therefore in software applications, it also ensures skyrocketing degrees of complexity. Greater complexity means more systemic seams, offering greater opportunities to those seeking to intrude and do harm. Not only must we adapt to the rhythm of civilian innovation, we have to accept the challenge of incorporating levels of protection for defense systems that go well beyond civilian standards.

In order to make new C4ISR capabilities available to unit structures immediately, our operational and system architectures have to be open to the insertion of new equipment and software, and we have to develop imbedded training modules that will allow operators and cadre to absorb and incorporate the needed skills quickly. This will also require an up-front investment in C4ISR infrastructure to ensure the necessary bandwidth. Without developing these pathways, the timely incorporation of off-the-shelf civilian technology is not possible.

Finally, we need to design into our training programs and command and control systems the mechanisms for mission rehearsal. With enough warning, tailored task forces can form and move to a training site for a detailed operational rehearsal in an environment that replicates the operational challenge they will face when deployed. Given warning time, this option remains the preferred method for ensuring mission success against a new mission profile in an unanticipated operational environment. If we develop simulations that can drive the C4ISR systems in a no-warning scenario, rehearsals of the leadership can be conducted as a unit deploys and conducts its movement into theater. If we design the command and control systems properly, then as units pack, stage, and deploy to the area of operations, leaders will use their actual command suites to rehearse plans and operations. In short- or no-warning scenarios, we would benefit from a higher state of training and the improvisation fostered by a greater ratio of leaders to led. Ideally this will generate a leadership ethic that fosters entrepreneurial decisionmaking. This level of readiness will promote our ability to conduct conventional warfighting tasks or to adapt quickly with little warning to the more abstract operational tasks required in unconventional settings in the face of asymmetrical threats applied idiosyncratically.

Asymmetry is an important concept, so long as we understand it. But operational idiosyncrasy—with its potential for shock and surprise from catastrophic mass effects or accelerating bad results, using reengineered civil or military systems—is an even more important challenge. Defeating these new threats requires us to restructure our decision systems for operations and to reorganize our structures for intelligence requirements, collection, and fusion. It requires hybrid teams of out-of-the-box thinkers, scientists, and military professionals

working under pressure together. It relies on matching agency expertise and access to the operational setting as a matter of national mandate. It requires a degree of operational and entrepreneurial latitude and initiative in conventional units similar to that exhibited in Afghanistan by our Special Forces teams and in Bosnia, Kosovo, and Iraq by conventional units. It requires a different definition of training readiness and units manned and trained and equipped for adaptation to new operational tasks on the fly. And all of these depend on a national doctrine for operations that subordinates agency autonomy to operational need and provides hybrid teams for intelligence analysis and fusion immediately at the joint headquarters at the operational level. Combined with what we now know of the art of operations, these improvements promise better results against asymmetry applied idiosyncratically, but only if in our operational art we can create leaders who can constantly look across the theater or area of operations in novel ways in search of the eccentric attack on a direction they did not know existed and which now threatens the integrity of their whole campaign.

NOTES

This article is based on oral presentations at the Belfer Center of the JFK School, Harvard University, and the Russian army's Combined Arms Academy (formerly the Frunze Academy) in the summer and fall of 2002.

1. Berkshire Hathaway, *2001 Annual Report*, p. 10.

2. Bernard Lewis, *The Assassins* (New York: Oxford Univ. Press, 1987).

3. The best treatments of the 1940 campaign remain William Shirer's *The Collapse of the Third Republic* (New York: Simon and Shuster, 1969), and Alistair Horne's *To Lose a Battle* (London: Papermac, 1990).

4. Federal Power Commission, *Report to the President by the Federal Power Commission the Power Failure in the Northeastern United States and the Province of Ontario on November 9-10, 1965* (Washington: Federal Power Commission, 6 December 1965), pp. 1-10.

5. ABC News.com, "Caught on Tape: U.S. Officials Say Bin Ladin Video Proves Sept. 11 Involvement," 13 December 2001, http://abcnews.go.com/sections/world/DailyNews/OBLtaperelease011213.html.

6. Rohan Gunaratna, *Inside Al Qaeda* (New York: Columbia, 2002), p. 64. See Chapter 2 for a discussion of al Qaeda's operational strategy. Gunaratna lays out not only al Qaeda's operational system but the manner in which it absorbs other terrorist organizations and NGOs to form a worldwide base for the actions of its teams of operators and their apprentices.

7. Peter L. Bergen, *Holy War Inc*. (New York: Free Press, 2001), p. 39.

8. In zoology, this process of forming a new organism from fragments of the old is called morphellaxis.

9. Hans Morgenthau, *Vietnam and the United States* (New York: Public Affairs Press, 1965). In this little book, written opposing our commitment in Vietnam, Morgenthau highlighted the psychological factor of strategic decisions, arguing that no amount of moral fervor and military efficiency could solve the problem if the strategy was not derived from a realistic assessment of the likelihoods of the environment and strategic interests. Though the parameters are different in this case, his message of clarity and getting the strategy right is still apt.

10. Warren Bennis and Burt Nanus, *Leaders* (New York: HarperCollins, 1997), pp. 102-40. Bennis and Nanus provide a useful construct for understanding how social architecture or culture in an organization shapes meaning and controls behaviors. In an operational setting, social architecture controls how the members of the team define information and fuse it into the essential grist for decision. See also Clayton M. Christensen, *The Innovator's Dilemma* (New York: Harper Business, 2000), pp. 29-56, for a related concept, value networks which can impede innovation. See also Rosabeth Moss Kantor, "Creating the Culture for Innovation," in *Leading for Innovation*, ed. Frances Hesselbein, Marshall Goldsmith, and Iain Somerville (San Francisco: Jossey Bass, 2002), pp. 73-85. For the quotation cited, see Herbert Simon, *Administrative Behaviour* (New York: Free Press, 1997), p. 292; see also the accompanying discussion on pp. 278-95.

11. Gretchen Hyman, "The Dark Side of Moore's Law," 7 August 2002, http://siliconvalley.internet.com/news/article.php/1442041.

12. C4ISR is an acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.